IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

United States of America, Plaintiff, vs. James Lee Thompson, and Janine May Edwards, Defendants.	))))))))))	**ORDER DENYING MOTIONS TO SUPPRESS** Case No. 1:21-cr-190

Before the Court is Defendant James Thompson's motion to suppress filed on September 12, 2022. See Doc. No. 51. The Government filed response in opposition to the motion on September 26, 2022. See Doc. No. 57. On October 18, 2022, Defendant Janine Edwards joined in the motion. See Doc. No. 60. The Government filed a response in opposition to Edward's motion on November 1, 2022. See Doc. No. 65. A hearing on the motions was held on November 15, 2022. The Government filed a post-hearing brief on December 20, 2022. See Doc. No. 77. Thompson filed a post-hearing brief on January 12, 2023. See Doc. No. 79. For the reasons set forth below, the motions are denied.

I. BACKGROUND

The Court held a suppression hearing on November 15, 2022. Five law enforcement officers testified at the hearing: Special Agent James Shaw from the North Dakota Bureau of Criminal Investigation, North Dakota Parol and Probation Officer Ashley Gawryluk, Detective Travis Leintz from the Dickinson, North Dakota Police Department, Detective Samantha Okke from the Dickinson, North Dakota Police Department, and Special Agent Matt Hiatt from the North Dakota

Bureau of Criminal Investigation. The factual background is derived from their testimony, as well as the law enforcement reports, affidavits, and other documentation in the record. See Doc. Nos. 55, 57-1 through 57-7, 62, and 73.

Sometime prior to May 2, 2021, Snapchat[1] flagged a single image uploaded to a Snapchat account through a specific internet protocol (IP) address. The image was identified as apparent child pornography using hash value matching technology.[2] The image was not viewed by Snapchat employees. **The image had been uploaded to a publicly viewable space**. On May 2, 2021, Snapchat submitted cybertip number 89705555 to the National Center for Missing and Exploited Children (NCMEC) and forwarded the suspected image to the NCMEC as required by 18 U.S.C. § 2258A. See Doc. No. 70. The cybertip included the account holder's IP address, email address, and username.

On May 27, 2021, the NCMEC forwarded the cybertip and the image to the North Dakota Bureau of Criminal Investigation ("BCI"). NCMEC staff did not view the image. BCI Special Agent Jesse Smith received the cybertip and viewed the publically viewable image without obtaining a search warrant. He determined the image was that of a nude female age 12-15 and appeared to be child pornography. The IP address associated with the Snapchat upload was registered to to Consolidated Telecom in Dickinson, North Dakota. Special Agent Smith

[1]Snapchat is a social messaging service that allows users to send photographs and videos that automatically delete a few seconds, usually ten, after being viewed by the recipient.

[2]"A hash value is (usually) a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value. Some consider a hash value as a sort of digital fingerprint." United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016). Hash values assigned to known child pornography images can be electronically compared to images uploaded through an electronic service provider and flagged if the hash values match. Id.

subpoenaed the internet service provider (Consolidated Telecom) and learned that the IP address belonged to James Lee Thompson, who had a Dickinson, North Dakota, address and was a registered sex offender. The email (onemorerep1981@gmail.com) associated with the Snapchat account that uploaded the image was the same as that associated with the Consolidated Telecom account.

On June 4, 2021, the BCI forwarded cybertip number 89705555 to Detective Samantha Okke of the Dickinson Police Department for further investigation. Detective Okke, without a search warrant, reviewed the publically viewable image and determined it was child pornography. Detective Okke then ran a records check on Thompson and determined he was a registered sex offender currently on probation with North Dakota Parole and Probation for offenses against children. Thompson was classified as a lifetime registrant with moderate risk. Thompson's probation officer was Ashley Gawryluk. The email address listed on his sex offender registration matched the email address associated with the suspect Snapchat account and the Consolidated Telecom account. The terms and conditions of Thompson's probation included a search clause.

Detective Okke consulted with state Probation Officer Gawryluk and learned that Thompson was prohibited from accessing social media or setting up internet service without authorization from his probation officer and that he did not have such permission. On July 20, 2021, Probation Officer Gawryluk requested Detective Okke assist her in searching Thompson's cell phone based upon her suspicion that Thompson had violated the terms and conditions of his state probation related to the

Snapchat upload.[3]

On July 21, 2021, Detective Okke and Detective Leintz conducted a sex offender compliance check on Thompson at the Dickinson Public Safety Center as part of a regularly scheduled check of all sex offenders in the Dickinson area. Thompson was placed in an interview room where he was read his Miranda rights and agreed to be interviewed. During the interview, Thompson made a number of incriminating statements and admissions, including communicating with an adult female named "Janine." While the interview was occurring, Detective Lietz searched Thompson's cell phone. A text message string between Thompson and co-defendant Janine Edwards revealed multiple nude images of a prepubescent male child sent by Edwards to Thompson. The detectives determined the images were child pornography and Thompson admitted the images were used for sexual fantasy purposes. At this point the interview and search of the cell phone were terminated. The cell phone (Samsung Galaxy 21) was seized and a state search warrant for the phone was requested. Thompson was arrested.

On July 22, 2021, Detective Okke received a search warrant for Thompson's cell phone. The subsequent search of the phone produced an incriminating text message thread between Thompson and Edwards, along with nude images of a male child sent by Edwards to Thompson.

On July 22, 2021, BCI Special Agent Matthew Hiatt obtained and executed a search warrant for Edwards's home, person, and digital devices. Edwards was home at the time of the search. Her

[3]There was a valid search clause provision imposed on Thompson in connection with his state conviction for luring minors by computer. The search clause provided as follows: "Submit the Defendant's person, place of residence and vehicle, or any other property to which the Defendant has access, wherever they may be found, to search and seizure, with or without a search warrant at any time of day or night by any parole or probation officer or any law enforcement officer at the direction of a parole or probation officer." See Doc. No. 69-3, p. 4. The Defendant had no reasonable expectation of privacy for searches conducted of his cell phone or Snapchat account.

cell phone was seized during the search of her home. Edwards was Mirandized and agreed to be interviewed. Edwards made a number of incriminating statements during the interview.

On July 23, 2021, Special Agent Hiatt conducted a follow-up interview with Edwards. Prior to the follow-up interview, Edwards was read her Miranda rights and agreed to be interviewed. During the follow-up interview, Edwards made additional incriminating statements.

On October 6, 2021, Thompson and Edwards were indicted in federal court. The indictment charges Thompson with one count of sexual exploitation of a child in violation of 18 U.S.C. §§ 2251(a), 2251(e), and 3559(e); one count of receipt of images depicting the sexual exploitation of children in violation 18 U.S.C. §§ 2252(a)(2), 2252(b)(1), and 3559(e); and one count of commission of a felony offense involving a minor when required to register as a sex offender in violation of 18 U.S.C. § 2260A. Edwards was charged with one count of sexual exploitation of a child in violation of 18 U.S.C. §§ 2251(b) and 2251(e) and one count of distribution of images depicting the sexual exploitation of children in violation 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1).

II. LEGAL DISCUSSION

Thompson contends that the warrantless viewing of the image flagged by Snapchat and forwarded to the NCMEC, which became the subject of a cybertip provided to North Dakota law enforcement officers, violated the Fourth Amendment and requires suppression of that image and all evidence derived from the warrantless viewing. The Government contends Thompson cannot demonstrate a subjective expectation of privacy in his Snapchat upload that society is willing to recognize as reasonable. Specifically, the Government contends the upload was made to a public

space, the Snapchat terms of service prohibit child pornography, and also state all such instances will be turned over to law enforcement.

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The purpose of the Fourth Amendment is to safeguard the privacy and security of the people against arbitrary invasions by governmental officials. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018). "Searches conducted without a warrant are per se unreasonable, subject to a few well-established exceptions." United States v. Hill, 386 F.3d 855, 858 (8th Cir. 2004).

As a general rule, the burden of proof is on the defendant who claims a Fourth Amendment violation has occurred and seeks to suppress evidence. Carter v. United States, 729 F.2d 935, 940 (8th Cir. 1984); United States v. Shipton, 5 F.4th 933, 936 (8th Cir. 2021). In the case of a warrantless search, the government bears the burden of establishing an exception to the warrant requirement. Id.; United States v. Kennedy, 427 F.3d 1136, 1140 (8th Cir. 2005); Hill, 386 F.3d at 858; United States v. Bruton, 647 F.2d 818 (8th Cir. 1981).

A. REASONABLE EXPECTATION OF PRIVACY

"The defendant moving to suppress bears the burden of proving he had a legitimate expectation of privacy that was violated by the challenged search." United States v. Muhammad, 58 F.3d 353, 355 (8th Cir. 1995); United States v. Pierson, 219 F.3d 803, 806 (8th Cir. 2000); United States v. Gomez, 16 F.3d 254, 256 (8th Cir.1994). This test is often referred to as the *Katz* inquiry and involves two discrete questions. Smith v. Maryland, 442 U.S. 735, 740 (1979); Katz

v. United States, 389 U.S. 347, 351-52 (1967). The defendant must demonstrate: (1) a subjective expectation of privacy in the place or objects searched, that is whether the person has demonstrated through his conduct that he seeks to preserve something as private; and (2) that the subjective expectation of privacy is one that society is prepared to recognize as objectively reasonable under the circumstances. Smith, 442 U.S. at 740; Muhammad, 58 F.3d at 355.

In analyzing whether Thompson had a subjective expectation of privacy in the image he uploaded to his Snapchat account that is objectively reasonable it is helpful to understand what Snapchat is and how it works. The Supreme Judicial Court of Massachusetts recently described Snapchat as follows:

> Snapchat allows users to share text, photographs, and video recordings, collectively known as "snaps." Snaps may be shared either as "direct snaps" or as "stories." Direct snaps are sent directly to another user's inbox, remain visible for ten seconds or less after they are opened, and can be viewed only once. Stories, on the other hand, by default are shared with a larger audience, remain visible for up to twenty-four hours, and can be continuously replayed. Either type of snap can be preserved if the recipient takes a screenshot or otherwise records the content by some other technology external to Snapchat.
>
> Snapchat accounts can be configured as either "public" or "private." When users initially create a Snapchat account, by default it is private, and the user must explicitly choose to make it public.
>
> Stories posted to public accounts are visible to all members of the public, whereas stories posted to private accounts by default are visible only to individuals that the user chooses to add as "friends." A user can add friends in one of three ways: "(1) by allowing Snapchat to access his or her phone's address book and add users who have registered using that contact information; (2) by manually inputting his or her friends' usernames; or (3) by approving other users who have requested to add the user."

Commonwealth v. Carrasquillo, 179 N.E.3d 1104, 1109 (2022) (internal citations omitted).

In this case, Thompson submitted no evidence as to whether his Snapchat account was

public or private, or the circumstances surrounding his upload of the publically viewable image in question which matched the hash-value assigned to a known image of child pornography. Thompson did not call any witnesses at the hearing that was held on his motion to suppress or submit any affidavits or declarations in support of the motion. It is well-established that the burden is on Thompson to demonstrate, through his conduct, that he had an actual subjective expectation of privacy in the image he uploaded on Snapchat. Shipton, 5 F.4th at 936. The only evidence in the record relevant to this inquiry is the Cybertip submitted by Snapchat to the NCMEC that positively indicated the entire contents of the uploaded file were publicly available. See Doc. No. 57-1. Nothing in the record contradicts this statement. Thompson has failed to carry his burden of demonstrating a subjective expectation of privacy in the image he uploaded.

Even if Thompson had demonstrated a subjective expectation of privacy, the Eighth Circuit Court of Appeals has repeatedly held that a defendant has no objectively reasonable expectation of privacy in files he shares on a public network or in an online space accessible by the public. Shipton, 5 F.4th at 936; United States v. Hoeffener, 950 F.3d 1037, 1044 (8th Cir. 2020) ("A defendant has no legitimate expectation of privacy in files made available to the public through a peer-to-peer file-sharing networks."). An individual does not have a reasonable expectation of privacy in information voluntarily turned over to third parties. See United States v. Miller, 425 U.S. 435, 442-43 (finding no expectation of privacy in financial records held by a bank); Smith, 442 U.S. at 745 (finding no expectation of privacy in records of dialed telephone numbers conveyed to telephone company). This is true even if the person believes the information will only be used for a limited purpose. Carpenter, 138 S. Ct. at 2216. Consequently, government officials are free to

obtain such information revealed to third parties without triggering the Fourth Amendment. Id. However, this third party doctrine is not without limits. See Carpenter, 138 S. Ct. at 2217 (finding individuals maintain a reasonable expectation of privacy in the record of their movements as captured by cell-site location information); United States v. Jones, 565 U.S. 400, 430 (2012) (finding a reasonable expectation of privacy in the whole of a persons movements). The Court sees little difference between files made available to the public through a peer-to-peer network and files uploaded to a location on Snapchat that was open to the public. The Court finds Thompson has failed to demonstrate an objective expectation of privacy society is willing to acknowledge as reasonable.

B. PROPERTY INTEREST

The *Katz* test is not the only relevant inquiry. The Court must also consider whether the government has physically intruded upon "private property for the purpose of obtaining information." United States v. Jones, 565 U.S. 400, 404-06 (2012) (finding the government violated the Fourth Amendment when it placed a GPS location device on an automobile to monitor its movements because in doing it obtained location information by physically intruding upon an individual's "persons, houses, papers, and effects"). This Fourth Amendment formulation is much older than the *Katz's* "reasonable expectation of privacy" test and is rooted in a traditional understanding of property rights and the law of trespass. Id. at 405. The United States Supreme Court in *Jones* explained that a search occurred when the Government physically occupied private property (an automobile) for the purpose of gathering information. Id. at 404. The holding was

based upon a property-based view of the Fourth amendment and the law of trespass. Id. at 405. The Supreme Court further explained that the "*Katz* reasonable-expectation-of-privacy has been *added to*, not *substituted for*, the common-law trespassory test." Id. at 409. In other words, "government conduct can constitute a Fourth Amendment search *either* when it infringes on a reasonable expectation of privacy *or* when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effects") for the purpose of obtaining information." United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016).

The Court is unpersuaded that *Jones* changes the result in this case. Unlike *Ackerman* which involved an email between the defendant and a lone recipient which the Tenth Circuit described as presumptively private correspondence, this case involves the upload of a single image and nothing more, **to a publicly viewable space**. There was no Government intrusion on a constitutionally protected space or thing because the image, a "paper or effect" in constitutional parlance, was no longer private because it was open to the public. The publicly viewable spaces on the internet cannot be considered constitutionally protected spaces for Fourth Amendment purposes and thus there was no trespass in the sense contemplated by *Jones*. See Shipton, 5 F.4th at 936 (concluding nothing in *Jones* calls into question the well-established principle that there can be no reasonable expectation of privacy in materials shared on a public network).

III. CONCLUSION

The Government need not avert its eyes from material an individual places in the public realm. The Court concludes that Thompson did not have a reasonable expectation of privacy in the

image he uploaded on Snapchat and thus no search, at least in the constitutional sense, occurred when law enforcement officials later viewed that image without first obtaining a search warrant. Having determined that Thompson did not have reasonable expectation of privacy in the images he uploaded to a publicly viewable space on Snapchat, Edwards' motion necessarily fails as well. In addition, Edwards motion would fail in its own right based upon a lack of standing. See United States v. Gomez, 16 F.3d 254, 256 (8th Cir. 1994) (noting Fourth Amendment rights are personal, cannot be asserted vicariously, and a defendant lacks standing where she has no sufficiently close connection to the place or objects searched).

The Court has carefully reviewed the entire record, the parties' arguments, the evidence presented at the suppression hearing, and the relevant case law. For the reasons outlined above, the motions to suppress (Doc. Nos. 51 and 60) are **DENIED**.

IT IS SO ORDERED.

Dated this 26th day of January, 2023.

/s/ Daniel L. Hovland
Daniel L. Hovland, District Judge
United States District Court